 Recibido: 22.9.25 / Aprobado: 27.11.25

TUTELA DE LA INFORMACIÓN PERSONAL Y LAS REDES SOCIALES EN CHILE, DE CARA A LA NUEVA LEY SOBRE LA PROTECCIÓN DE DATOS PERSONALES*

PROTECTION OF PERSONAL INFORMATION AND SOCIAL NETWORKS IN CHILE, IN THE FACE OF THE NEW LAW ON THE PROTECTION OF PERSONAL DATA

*Francisco Javier Sanz Salguero***

RESUMEN: Este artículo tiene por objeto realizar una aproximación a los avances de la nueva Ley sobre la Protección de Datos Personales, en su relación con las redes sociales. Para estos efectos, se lleva a cabo un trabajo de comparación entre el nuevo estatuto legal y la Ley 19.628 de 1999 acerca de Protección de la Vida Privada, labor que incluye la identificación de deficiencias en la Ley 19.628 en su vínculo con las redes informáticas, el análisis de la expectativa de privacidad, y los progresos en el tratamiento de la información personal dentro de las redes sociales logrados con la nueva normativa.

Palabras clave: Derecho a la protección de los datos personales, Derecho a la protección de la vida privada, nueva Ley sobre la Protección de Datos Personales, redes sociales.

ABSTRACT: *This article aims to make an approach to the progress of the new Law on the Protection of Personal Data, in its relationship with social networks. For these purposes, a comparison work is carried out between the new legal statute and Law 19,628 of 1999 on the Protection of Private Life, work that includes the identification of deficiencies in Law 19,628 in its link with computer networks, the analysis of the expectation of privacy, and the progress in the treatment of personal information within social networks achieved with the new regulations.*

Keywords: Right to protection of personal data, Right to protection of private life, new Law on the Protection of Personal Data, social networks.

---

*Este trabajo es parte del proyecto Fondecyt de Iniciación Nº 11221089, "Desafíos para la modernización de la Ley Nº 19.628 de 1999, de cara al alcance extraterritorial del Reglamento General de Protección de Datos de la Unión Europea GDPR", financiado por la Agencia Nacional de Investigación y Desarrollo ANID (Chile).

**Doctor en Derecho Pontificia Universidad Católica de Valparaíso (Chile). Abogado, Universidad Externado de Colombia. Académico investigador, Universidad Santo Tomás, Santiago, Chile. Correo electrónico: fjsanzsalguero@hotmail.com. DOI: https://orcid.org/0000-0002-3082-3863.

I. INTRODUCCIÓN

En una perspectiva global, en especial desde los inicios de la llamada *época de la información*[1], el interés por el tratamiento de la privacidad y los datos personales ha sido permanente. Su protección se debe estudiar de forma simultánea con los avances alcanzados en el ámbito de la transformación digital (proceso enraizado en la innovación tecnológica que trae aparejada nuevas oportunidades, pero que a la vez puede generar, reproducir o reforzar desigualdades)[2], elementos que, en conjunto, han tenido un impacto en la modificación de la conducta de los individuos dentro del espectro de internet, efecto que incluye estructuras informáticas como las redes sociales. Esta situación determina la importancia de la tutela de la información personal en el escenario actual, circunstancia reconocida por el Derecho continental europeo con la aprobación y reciente aplicación (2018) del Reglamento General de Protección de Datos de la Unión Europa (en adelante GDPR, por sus siglas en inglés)[3], legislación más avanzada en esta materia[4]. En el caso chileno, el interés por el resguardo de la privacidad y los datos personales se manifiesta en una evolución legal, con tres hitos clave. En primer lugar, tenemos la aprobación de la Ley Nº 19.628 de 1999, acerca de protección de la vida privada (en adelante LPD[5]), estatuto que en su trámite parlamentario surgió bajo la pretensión de tutelar la vida privada, pero que luego de un complejo debate legislativo terminó concentrándose en la protección de los datos personales. En segundo término, observamos la modificación del artículo 19 numeral 4 de la Constitución, que reconoce el carácter de Derecho Fundamental a la protección de la información personal. En tercer lugar, y como reforma a la LPD, tenemos la Ley 21.719 que "regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales" (en adelante Nueva LPDP), aprobada por el Parlamento chileno[6] y publicada el 13 de diciembre del 2024, estatuto cuya vigencia está diferida hasta el 1º de diciembre del 2026.

Teniendo en cuenta las debilidades atribuidas a la LPD y los efectos de la Nueva LPDP, definir el estado de la cuestión del tratamiento de los datos personales incorporados en las redes sociales, se configura en el objetivo central de la presente investigación. El examen de este asunto se sustenta a propósito de los progresos generados con las transformaciones tecnológicas y la modificación del comportamiento de los individuos en

---

[1]PÉREZ, 2013, 48.

[2]SANZ, 2025, 4.

[3]Reglamento General de Protección de Datos (UE) Nº 2016/679. Publicado en el Diario Oficial de las Comunidades Europeas el 27 de abril de 2016.

[4]MILANÉS, 2017, 20.

[5]Publicada en el Diario Oficial el 28 de agosto de 1999.

[6]Aprobación generada el 26 de agosto del 2024.

la esfera de las estructuras informáticas. Fijando como horizonte la identificación de los avances logrados con la aprobación de la Nueva LPDP, en la primera etapa del trabajo abordamos los principales hitos legales en materia de protección de los datos personales, y los problemas surgidos en ese proceso de construcción normativa. Esta labor se realiza con el fin de justificar la redacción de la Nueva LPDP. En una segunda fase, en la investigación se realiza un panorama general de la noción red social, revisando además los principales elementos que estructuran a estas redes y su vínculo con la privacidad y los datos personales. Como un aporte complementario, el capítulo subsiguiente examina el tratamiento jurisprudencial de la llamada expectativa de privacidad asociado a la esfera de las redes sociales, por parte de la Corte Suprema chilena. En la etapa final de la investigación se lleva a cabo una labor de comparación entre la LPD y la Nueva LPDP, con énfasis en la situación de las redes sociales, esfuerzo que permitirá identificar los avances de la nueva normativa respecto del tratamiento de la información personal en estas plataformas informáticas.

Con las anteriores premisas, el documento estudia por primera vez los efectos de la Nueva LPDP en el ámbito de las redes sociales, trabajo en donde descansa su carácter novedoso que contribuye a las ciencias jurídicas. El producto de este esfuerzo será de utilidad tanto para las autoridades del Estado (incluyendo legisladores y demás funcionarios) como para los investigadores y académicos chilenos y extranjeros, y al público en general. Finalmente, en cuanto a su estructura la investigación está dividida en una introducción, cuatro apartados principales y las conclusiones.

II. DE LA PROTECCIÓN A LA VIDA PRIVADA O PRIVACIDAD A LA TUTELA DE LOS DATOS PERSONALES EN EL CASO CHILENO

En el escenario interno, comprender el tratamiento de la información personal y su relación con las redes sociales en el contexto de la Nueva LPDP, exige revisar el tratamiento legal otorgado al resguardo de la vida privada o privacidad. Como comentario inicial y para facilitar la lectura del documento, advertimos que utilizamos indistintamente las expresiones *vida privada* o *privacidad*, lo que se justifica observando la falta de univocidad en los contenidos que la literatura jurídica propone a estas figuras[7] (de hecho, Jijena estima que esta diferenciación parece carecer de efectos jurídicos en la legislación interna[8]), llegándose incluso al uso indistinto de las nociones de privacidad y vida privada en algunos modelos normativos (materia donde el estudio del derecho debe aún trabajar con el

[7]SANZ, 2018, 142.

[8]Este pensamiento no es nuevo, ya que vemos opiniones en ese sentido desde principios de la década de los 90 del siglo pasado. JIJENA, 1992, 37.

fin de formular definiciones claras de estos conceptos)[9]. Lo comentado, va aparejada a la dificultad de construir una definición precisa del derecho a la vida privada o derecho a la privacidad, proceso de redacción que, en palabras de Novoa, depende del régimen social, político y económico en el que se desarrolle[10].

En cuanto al tratamiento normativo, la preocupación por la tutela de la vida privada tiene un primer hito relevante con la promulgación en 1999 de la LPD, estatuto que en su trámite parlamentario surgió bajo la pretensión de resguardar la privacidad, pero que luego de un intenso trabajo legislativo terminó enfocándose en la protección de los datos personales[11]. Al respecto, compartimos la opinión de Anguita, quien reconoce la presencia de fallas en la técnica legislativa, y una "falta de claridad en torno a los objetivos del proyecto de ley como una efectiva tutela de los datos personales y derechos conferidos a sus titulares, como también a la operatividad de los principios que recoge el texto legal en definitiva promulgado como ley de la República"[12]. Las fallas atribuibles a la LPD no se limitan a su proceso de construcción legislativa. En este sentido, el incumplimiento de los compromisos adquiridos por el Estado chileno al momento de ingresar (el año 2009[13]) a la Organización para la Cooperación y el Desarrollo Económicos, OCDE, compromisos consistentes en la obligación de implementar las Directrices relativas a la protección de la privacidad y el flujo transfronterizo de datos personales, le valió al país ser objeto de advertencias por parte de este organismo[14]. Los problemas identificados, en conjunto, son factores que inciden en la naturaleza deficiente de la LPD. En un segundo hito, el año 2018 se modificó el artículo 19 numeral 4 de la Carta Política[15], otorgándose a la protección de datos personales un estatus iusfundamental. Precisamente, entre los argumentos esgrimidos durante el debate legislativo que generó

---

[9]De hecho, en la escena constitucional chilena la dificultad para distinguir estos conceptos tiene como ejemplo la redacción del actual artículo 19 Nº 4 de la Carta Política de 1980 (norma que reconoce "el respeto y protección a la vida privada y a la honra de la persona y su familia, y asimismo, la protección de sus datos personales"), proceso de confección normativa en el que se propusieron expresiones como "intimidad" y "privacidad", hasta llegar a la definitiva "vida privada". SANZ, 2013, 461-462.

[10]NOVOA, 2001, 43.

[11]En efecto y desde el punto de vista del tiempo utilizado en el desarrollo de la iniciativa, éste se inicia con la presentación de la moción parlamentaria formulada el 5 de enero de 1993, y culmina con la promulgación de la normativa ocurrida el 18 de agosto de 1999.

[12]ANGUITA, 2007, 277-278.

[13]En diciembre de 2009, 14 meses después de haberse iniciado el proceso de incorporación, el Consejo de la OCDE invitó a Chile a convertirse en su miembro número 31. SÁEZ, 2010, 108.

[14]VIOLLIER, 2017, 39.

[15]Reforma constitucional generada a través de la Ley Nº 21.096, de 5 de junio de 2018, que "Consagra el derecho a protección de los datos personales". Publicada en el Diario Oficial el 16 de junio del 2018.

aquella modificación constitucional, se plantea el carácter autónomo de la protección de la información personal respecto de la tutela de la vida privada[16]. Por último, un tercer hito clave en el ámbito del tratamiento legal interno lo representa la aprobación el año 2024 de la Nueva LPDP, texto que apunta a superar las anomalías atribuidas a la LPD.

Subrayando que no es la pretensión del presente trabajo hacer un examen exhaustivo de los derechos a la protección de la vida privada o a los datos personales, pero considerando necesarios los comentarios generales de este primer capítulo con el fin de justificar la creación de la Nueva LPDP, en la siguiente fase de la investigación efectuamos un panorama general de la noción "red social", junto con los principales elementos que configuran a estas plataformas tecnológicas y su vínculo con la privacidad y los datos personales. Igualmente abordamos el concepto de "expectativa de privacidad", dentro del esfuerzo de la doctrina por establecer criterios objetivos que permitan dar a conocer la existencia de un espacio de privacidad jurídicamente tutelado. A continuación, llevamos a cabo la labor propuesta.

III. ASPECTOS GENERALES DE LAS REDES SOCIALES Y SU IMPACTO EN EL TRATAMIENTO DE LA VIDA PRIVADA Y LOS DATOS PERSONALES

Se le reconoce a las redes sociales el carácter de estructuras formadas en la esfera de internet[17], sistemas en los que los individuos u organizaciones se conectan a partir de intereses o valores comunes. Teniendo en cuenta el volumen de la información que los individuos comparten en estas redes y su carácter heterogéneo (que abarca desde los pensamientos banales a posiciones políticas, pasando por las creencias religiosas y orientación sexual, por mencionar solo algunas áreas de interés), y agregando que muchas veces esa información incluye datos que identifican o hacen identificables a los individuos, ante el hecho que esa información queda a disposición de muchas personas es posible que se haga un uso poco

[16]La moción fundamenta la autonomía del derecho a la protección de datos citando, entre otros, argumentos de la jurisprudencia comparada y de la doctrina. Respecto de jurisprudencia comparada, tenemos un caso del Censo fallado por el Tribunal Constitucional Federal Alemán [Sentencia del Tribunal Constitucional Federal Alemán, BVerfGE65, 1 (1983)] y una sentencia del Tribunal Constitucional español [Sentencia del Tribunal Constitucional Español ("STCE") 292/2000]. Respecto de la doctrina, se tuvo en cuenta opiniones de autores como Enrique Rajevic y Humberto Nogueira. CONTRERAS, 2020, 90-91 y 93-94.

[17]A su vez, es posible identificar el "internet" como una gran red internacional de ordenadores, es decir, una red de redes o unión de diversas redes internacionales a un núcleo central. Como todas las redes, esta estructura permite compartir recursos: o sea, mediante el ordenador, establecer una comunicación inmediata con cualquier parte del mundo para obtener información acerca de un tema que nos interesa. DE LA CUADRA, 1996, 35.

adecuado de la misma, llegándose incluso a la afectación de derechos fundamentales[18]. La amenaza del mal uso de la información va de la mano con fenómenos como el *oversharing*[19] y el *sharenting*[20], situaciones originadas con el auge de las plataformas informáticas[21].

Acudiendo a definiciones más elaboradas, Agustinoy y Monclús identifican a la red social como "aquella plataforma tecnológica que permite a sus usuarios, mediante sus correspondientes perfiles, vincularse entre sí, creando sistemas cruzados e interactivos de generación y difusión de información"[22]. Desde otra perspectiva, el Grupo de Estudios del artículo 29 del Consejo de Europa las distingue como aquellas plataformas de comunicación en línea que permiten a los individuos crear redes de usuarios que comparten intereses comunes[23]. Entre tanto, la Agencia Española de Protección de Datos AEPD las define como los "servicios prestados a través de internet que permiten a los usuarios generar un perfil público, en el que plasmar datos personales e información de uno mismo, disponiendo de herramientas que permiten interactuar con el resto de usuarios afines o no al ser publicados"[24]. Con independencia de la noción que se adopte, en todas ellas se reitera la dupla individuo-difusión de la información propia, hipótesis que puede llevar aparejada la afectación de la vida privada o al derecho fundamental a la protección de los datos de carácter personal.

A partir de las anteriores definiciones, Escobar reconoce 3 elementos principales que configuran una red social, elementos de los que emergen las mayores vulneraciones a la privacidad o a los datos personales: comunicación, identidad e interconectividad. Mientras que el elemento "comunicación" indica que (gracias al deseo de querer comunicarse con otras personas) los usuarios de una red social exponen información personal, el elemento "interconectividad" hace referencia a que la comunicación al interior de las redes sociales se desarrolla de forma masiva, instantánea y recíproca[25]. Entre tanto, el factor del cual surgen las principales transgresiones contra el derecho al resguardo de la información personal, lo constituye el elemento "identidad", teniendo en cuenta que los datos personales que conforman nuestra personalidad son el medio de cambio para poder ingresar y participar en estos servicios: el exceso de contenido

[18]TORRES (2021), 221.

[19]Palabra inglesa que describe el hecho de compartir todo tipo de información personal, prácticamente sin límite.

[20]El *sharenting*, es la acción de los padres de compartir información pormenorizada de sus hijos en internet, mediante redes sociales.

[21]ORDÓÑEZ y CALVA, 2020, 115 y 117.

[22]AGUSTINOY y MONCLÚS, 2016, 20.

[23]Dictamen del Consejo de Europa 05/2009 sobre redes sociales en línea, adoptado el 12 de junio de 2009.

[24]SANZ, 2023, 7.

[25]ESCOBAR, 2023, 2.

vertido en este tipo de plataformas hace posible obtener una perspectiva general de la personalidad de determinado individuo, personalidad que está protegida como una proyección de su privacidad[26]. A la par con el amplio espectro de redes sociales de las que actualmente se dispone, las más usadas generan mayor amenaza a la vida privada o a la información personal[27]. El escenario anterior plantea una situación de más vulnerabilidad respecto de los datos de naturaleza personal, observando que los servicios de internet imponen a sus usuarios un conjunto de obstáculos (tanto en el momento de registro como en la participación y cancelación de la cuenta) con el propósito de que viertan la mayor cantidad de sus datos personales.

Finalmente, no obstante, el carácter autónomo atribuido al derecho a la protección de la información personal en relación con el resguardo de la vida privada (factor mencionado anteriormente), un tema de interés para la investigación lo constituye el tratamiento de la expectativa de privacidad asociada a las redes sociales. A este respecto, lo primero a comentar es que el desafío de elaborar una definición del derecho a la vida privada es un asunto vinculado con el carácter relativo que le caracteriza. Debido a esta relatividad, Herrera ha propuesto dirigir esfuerzos para establecer criterios objetivos que permitan dar a conocer la existencia o no de un espacio de privacidad jurídicamente protegido[28]. En este escenario, ese espacio de privacidad estará presente en caso de que exista una expectativa legítima de privacidad[29]. La "expectativa de privacidad"[30] del usuario[31]

---

[26]HERRERA, 2016, 93-95.

[27]De acuerdo con un reporte elaborado por *We are social*, Facebook sigue encabezando el listado de red social más utilizada (aunque se encuentra en una situación de declive). El mismo reporte destaca el fortalecimiento de plataformas como Tik Tok, Snapchat y Telegram, junto con el "impresionante" crecimiento para Reels. WE ARE SOCIAL (2022).

[28]HERRERA, 2016, 89.

[29]ESCOBAR, 2023, 6.

[30]A este respecto, mientras algunos autores defienden la concepción de la privacidad como el control del flujo de la información personal, otro sector de la doctrina ha señalado su desacuerdo con definir la privacidad atendiendo al control de la información [ya sea por considerarla una concepción muy ambigua (que habrá de delimitarse a base del tipo de información que merece protección o reserva), o por estimar que definir el derecho basado en las facultades de control del sujeto permite considerarlo como un derecho de propiedad de la información personal (concepción de la privacidad informacional que impediría una efectiva protección de la vida privada al generar expectativas inexistentes y distorsionar sus posibles amenazas)]. NIEVES, 2007, 100.

[31]Al concentrarnos en las tecnologías de la información y comunicación en internet, Schwartz estima que (desde una perspectiva escéptica acerca de la capacidad individual para controlar el flujo de información personal para el ejercicio de la llamada autodeterminación informativa), no obstante, que la conceptualización de la privacidad como un derecho de control sobre la información personal supone el reconocimiento y la existencia de un importante ámbito de autonomía individual, esta concepción no es satisfactoria, ya que conlleva una visión mercantilista de la privacidad cercana al derecho de propiedad intelectual, asociado al hecho que en el ámbito de las tecnologías de la información y comunicación (especialmente en

se aplicaría por los tribunales al momento de establecer los límites del derecho a la privacidad en los medios digitales que ofrecen redes sociales, hipótesis en la que la judicatura observa tres elementos: el grado de configuración del perfil, la cantidad de contactos y el perfil indexado a motores de búsqueda. En este sentido, la expectativa de privacidad será mayor en los casos donde opte por comunicarse mediante mensajería privada, su perfil tenga un número reducido de contactos, y no esté indexado a un motor de búsqueda, caso donde se confirma la intencionalidad del usuario de mantener ciertas áreas de su vida excluidas del conocimiento público[32]. Precisamente, la jurisprudencia chilena aborda la expectativa de privacidad asociada a la esfera de las redes informáticas, materia que examinamos a continuación.

IV. REDES SOCIALES Y TRATAMIENTO DE LA VIDA PRIVADA EN LA JURISPRUDENCIA NACIONAL, CON ÉNFASIS EN LA EXPECTATIVA DE PRIVACIDAD

A propósito de lo declarado por la jurisprudencia nacional, en este capítulo revisamos los criterios de la Corte Suprema chilena (en adelante CS) en materia de publicaciones en redes sociales, enfatizando en el tratamiento otorgado por ese tribunal a la expectativa de privacidad dentro del ámbito de estas redes informáticas.

Respecto de los criterios de la CS en relación con publicaciones en redes sociales y la resolución de acciones de protección constitucional[33] (teniendo en cuenta la competencia que le permite al tribunal conocer acciones de garantías de derechos fundamentales[34] con carácter definitivo[35]), la jurisprudencia de la Corte aborda el derecho al respeto y la protección de la vida privada, el derecho a la honra y el derecho a la protección de datos personales. Estas garantías de naturaleza iusfundamental, se hallan contenidas en el artículo 19 Nº 4 de la Carta Política. En este sentido y de acuerdo con Contreras y Lovera[36], el grueso de los argumentos de la CS se ha concentrado en la honra de los recurrentes, enfatizando además

internet) se registran importantes limitaciones para el control real de la información personal, principalmente por la complejidad técnica del medio y por la ausencia de información clara y disponible para los usuarios respecto de políticas de privacidad. SCHWARTZ, 2000, 820.

[32]HERRERA, 2016, 95-96.

[33]Acción reconocida en el artículo 20 de la Carta Política.

[34]Procesos constitucionales de tutela subjetiva.

[35]CONTRERAS y LOVERA, 2020, 91-95.

[36]CONTRERAS y LOVERA, 2021, 351.

en el reconocimiento implícito[37] del derecho a la imagen[38], sentencias en las que solo se cita genéricamente el respeto y protección de la vida privada, y no hay [salvo alusiones tangenciales, como ocurre con la sentencia rol n° 104785-2020 (considerando tercero) y la sentencia rol n° 125688-2020 (considerando cuarto)] un empleo del derecho a la tutela de datos personales.

Continuando con las opiniones de la CS, el tribunal también se encarga de la expectativa de privacidad asociada a la esfera de redes sociales específicas. Tomando como modelo la noción otorgada a esta expectativa por parte de la jurisprudencia de Estados Unidos, en particular el concepto desarrollado por el juez John M. Harlan dentro de la sentencia *Katz vs. United States*[39], los argumentos del alto tribunal chileno parten del supuesto que no cualquier expectativa de privacidad está jurídicamente protegida, siendo necesario que ella se encuentre objetivamente justificada sobre la base de las circunstancias concretas del caso, y que la sociedad esté dispuesta a protegerla[40]. En este sentido, las decisiones de la CS han examinado casos que involucran plataformas digitales como Facebook, Grindr y WhatsApp.

En relación con la casuística vinculada a Facebook (en un cambio de opinión respecto del enfoque observado en sentencias anteriores[41]), la reciente jurisprudencia de la CS indica que, desde el momento que el titular de la información la publica en esta red social (información que se comparte con todos sus contactos), se genera una renuncia tácita a que la misma se mantenga en una esfera privada o íntima, pues una vez difundida no es posible controlar el flujo informativo ni evitar que personas que tuvieron acceso a dicha información la compartan con otras[42].

Respecto de Grindr, aplicación tipo red social dirigida especialmente a la comunidad homosexual, la jurisprudencia de la CS descartó que ingresar a una red social más o menos abierta a un grupo indeterminado de

---

[37]En efecto, el derecho a la propia imagen no se encuentra expresamente reconocido en la Constitución.

[38]Derecho a la imagen resguardado por la Constitución y la acción de protección, según lo expresa el alto tribunal en las sentencias rol. n° 58531-2020, c. 4 y rol. n° 90737-2020, c. 4.

[39]MARIKO, 2017, 1601.

[40]ESCOBAR, 2023, 19.

[41]En efecto, en decisiones previas que involucraban a esta red social, para la CS la configuración de privacidad que el usuario seleccionara era el elemento clave. De esta forma, si el nivel de exposición era público, el tribunal descartaba la existencia de una expectativa legítima de privacidad. Al contrario, si el nivel de exposición era privado, el reclamante tenía una base sólida para demandar el reconocimiento de una expectativa legítima de privacidad. Esta opinión del tribunal se deduce de sentencias como el rol n° 5322-2012 (puntualmente del voto disidente del Ministro Sergio Muñoz), rol n° 1067-2018 y rol n° 42718-2021.

[42]Justamente tenemos la sentencia rol n° 12185-2022 de la CS, decisión que confirmó a su vez una sentencia dictada por la Corte de Apelaciones de Puerto Montt (sentencia rol n° 1428-2021). ESCOBAR, 2023, 16.

personas (individuos que comparten un cierto gusto, tendencia o afición), constituye una diligencia intrusiva que requiera autorización judicial por afectar el derecho a la privacidad de sus miembros[43]. Esta opinión de la Corte tiene en cuenta que quienes hacen parte de esta aplicación informática han aceptado voluntariamente compartir cierta información en la red[44].

A diferencia de lo que ocurre con Facebook y Grindr, teniendo en cuenta que la plataforma de WhatsApp establece un sistema de seguridad por defecto (sistema capaz de impedir que terceros, incluyendo a la misma plataforma, accedan al contenido de las conversaciones allí mantenidas), la opinión de la CS respecto de esta aplicación de mensajería instantánea permite fundar una expectativa de privacidad con base en el siguiente argumento: la posibilidad de la aplicación para enviar y recibir todo tipo de mensajes y documentos (incluyendo imágenes, videos y audios, así como llamadas y videollamadas), se soporta en la existencia de una seguridad predeterminada consistente en un cifrado de extremo a extremo, capaz de proteger lo transmitido[45]. Como consecuencia, para el tribunal los usuarios de esta red social pueden legítimamente confiar en que la información por ellos compartida en sus conversaciones no será difundida por personas ajenas a ellas[46].

Finalmente, alcanzar los objetivos de la presente investigación exige contrastar los contenidos de la LPD y la Nueva LPDP, con acento en la situación de las redes sociales. Este esfuerzo nos permitirá identificar los avances de la nueva normativa respecto del tratamiento de la información personal en esas plataformas informáticas. En el siguiente capítulo nos enfocamos en la labor planteada.

V. TRATAMIENTO DE LOS DATOS PERSONALES Y LAS REDES SOCIALES: ANÁLISIS COMPARATIVO ENTRE LA LPD Y LA NUEVA LPDP

Teniendo en cuenta las fallas atribuidas a la LPD, surge el desafío de establecer cuáles de estas deficiencias son subsanadas con la nueva LPDP. Desde esta perspectiva, a partir de una labor de contraste entre la ley anterior y la norma recientemente aprobada, el presente capítulo aborda las principales amenazas en materia de protección de los datos personales vertidos en las redes sociales, en el marco de aplicación de la LPD. Simultáneamente, se identificarán los cambios generados con la nueva LPDP con el fin de enfrentar estas amenazas. En el trabajo planteado, la situación de la información personal en su vínculo con las redes sociales

[43]Puntualmente, tenemos las sentencias rol n° 16921-2018 y rol n° 20441-2018.
[44]ESCOBAR, 2023, 16.
[45]Sentencia rol n° 71491-2021, considerando séptimo.
[46]ESCOBAR, 2023, 21.

se examina desde diversas materias, temas que incluyen el tratamiento de los datos de los menores de edad; los efectos de la creación del organismo con la capacidad de regular el tratamiento de la información; el "consentimiento" como requisito de licitud para el tratamiento de los datos personales; y los efectos de una inadecuada configuración de privacidad por parte del usuario al momento de efectuarse el registro en una red social, con énfasis en el concepto de "fuente de acceso público". Con este análisis y previo al marco de conclusiones correspondiente, terminamos la presente investigación.

a. *TRATAMIENTO DE LOS DATOS PERSONALES DE LOS MENORES DE EDAD Y LAS REDES SOCIALES*

Como una anomalía legal de carácter relevante, la LPD no otorga expresamente un grado de protección especial a los datos de los menores de edad, incluyendo aquellos que identifican directamente o hacen identificable a un individuo[47]. Esta falla tiene efectos en el ámbito de las redes sociales. Son diversos los argumentos que justifican la incorporación de esta tutela en la esfera normativa, teniendo en cuenta el impacto de internet y la forma en la que se llevan a cabo las distintas prestaciones de servicios por ese medio tecnológico.

En efecto, la publicación de fotografías o videos en las redes sociales puede influir en la identidad del individuo al que pertenece la imagen divulgada y, en el caso de niños y adolescentes, al crecer y convertirse en adultos jóvenes, corren el riesgo de encontrarse frente a una identidad digital (identidad entendida como el conjunto de información personal que se hace pública en internet, y que caracteriza a una persona o institución a partir de lo que es o dice ser en la red[48]) ya existente que podría no reconocer, o con la que podría no identificarse[49]. En este contexto, lo atendible es incorporar al ordenamiento jurídico dos exigencias: en primer lugar, el consentimiento de los padres o de aquellas personas a cargo del cuidado de los menores para poder realizar tratamiento de datos sensibles y, en segundo lugar, el mismo consentimiento para el tratamiento de datos personales o datos sensibles de los niños menores de 14 años o niñas menores de 12 años (según la distinción formulada por el Código Civil[50]).

---

[47]Respecto de los énfasis que plantea SCAFFIDI en la Unión Europea, acerca de la relación entre las redes informáticas y los datos personales, tenemos el caso de las fotografías o videos subidos a las *redes sociales* (una conducta muy frecuente entre los menores internautas), debido a que los efectos de la publicación de las imágenes no son necesariamente inmediatos, sino que pueden surgir incluso después de mucho tiempo. SCAFFIDI, 2021, 312.

[48]HUERTA y otros, 2021, 48.

[49]SCAFFIDI, 2021, 283.

[50]Artículo 26, Código Civil chileno.

Esta propuesta de incorporación legal apunta a que los menores de 18 años y mayores de 14 o 12 puedan desarrollar sus actividades en internet de forma más segura (teniendo en cuenta los peligros que han surgido en el marco de los avances de la actual era digital[51]), cumpliendo con el rol recreativo y educacional de la red (debido a que la industria no requiere de datos sensibles para la prestación de sus servicios), estableciéndose así un nivel de seguridad superior para aquellos datos personales sensibles que puedan ser requeridos o entregados por estos menores, los que deben contar con la autorización de sus padres o tutores[52]. En sintonía con las anteriores propuestas, Serrano y Martínez han subrayado la importancia de contar con un mecanismo confiable que permita verificar la edad de quien se registra en una plataforma, al momento de crearse el perfil en una red social[53].

En consonancia a las propuestas anteriores y a diferencia de lo que ocurre con la LPD, la Nueva LPDP en su artículo 16 quáter da tratamiento expreso a los datos personales "relativos a los niños, niñas y adolescentes", tratamiento que se encuentra basado en dos directrices: la atención al interés superior de estos, y el respeto por su autonomía progresiva (entendida esta última como la capacidad de los niños, niñas y adolescentes de ejercer sus derechos, a medida que se desarrollan mental y físicamente[54]). A partir del cumplimiento de estas dos premisas, el señalado artículo indica que para tratar la información personal de los niños y niñas (es decir los menores de 14 años, sin hacer distinción por género[55]) se requiere el consentimiento otorgado por sus padres o representantes legales, o por quien tiene a su cargo el cuidado personal.

Aunque el artículo aborda expresamente la situación de los datos personales de los adolescentes (incluyendo en este rango etario a los mayores de 14 y menores de 18 años), se limita a indicar que estos datos en particular podrán ser tratados "de acuerdo con las normas de autorización previstas en esta ley para los adultos", estableciendo una excepción a esta regla: solo es posible el tratamiento de la información personal sensible de los adolescentes menores de 16 años, cuando así lo consientan sus padres o representantes legales, o quien tiene a su cargo el cuidado personal del menor. Adicionalmente, y con un sentido innovador, en la norma se destaca la obligación impuesta a los "establecimientos educacionales y

[51]Observando que este grupo etario suele ser víctima de redes de delincuencia organizada, especializada en tráfico de personas, prostitución, trata de blancas, tráfico de órganos, estupro o almacenamiento de material pornográfico infantil, entre otras conductas. DIARIO CONSTITUCIONAL, 2021.

[52]ONG META, 2012, 18–21.

[53]SERRANO y MARTÍNEZ, 2021, 597.

[54]RIVERA, 2022, 147.

[55]En efecto, acá no se tienen en cuenta las diferencias etarias entre hombre y mujer del artículo 26 del Código Civil chileno.

de todas las personas o entidades públicas o privadas que traten o administren datos personales de niños, niñas y adolescentes", de "velar por el uso lícito y la protección de la información personal" que concierne a los menores de edad.

En conclusión, con la finalidad de un disfrute más seguro de las actividades desarrolladas en el espectro de internet (lo que incluye la participación de las redes sociales), el consentimiento de los padres o representantes se convierte con la Nueva LPDP en el mecanismo para alcanzar un mayor nivel de protección de los datos personales de niños, niñas y adolescentes. Lo anterior, combinando de forma armónica el interés superior de los menores de edad con la autonomía que van adquiriendo en la medida que desarrollan su identidad.

b. *CREACIÓN DE LA AGENCIA DE PROTECCIÓN DE DATOS PERSONALES APDP*

Otra crítica formulada a la LPD era la falta del reconocimiento de una autoridad con la capacidad de regular el tratamiento de la información personal. Gracias a esta ausencia, Chile no contaba con un organismo independiente (dotado de autonomía técnica y funcional) y especializado en materia de privacidad y protección de datos personales, investido de potestades de fiscalización, coerción y prevención[56]. Igualmente, existía una autoridad capaz de conciliar la tutela de datos con la transparencia en lo público[57]. De esta manera, en el país suramericano la tutela de la información personal descansaba, esencialmente, sobre el impulso de los particulares para poner en marcha los mecanismos institucionales (administrativos y judiciales) de protección de esos datos, aspecto asociado a la decisión y capacidad técnica y económica de esos particulares para sustanciar procedimientos, ya sea contra la Administración del Estado o contra empresas o individuos especializados en tecnologías de la información (factor que se integra a las plataformas informáticas)[58]. En consecuencia, frente a la utilización indebida de su información personal (hipótesis que incluye el mal uso de la información incorporada en las redes sociales), la alternativa para el titular de los datos era la presentación de una demanda ante la jurisdicción ordinaria, con todos los costos y complejidades que llevan aparejados estos procedimientos[59]. Acerca de este último aspecto, Herrera plantea el siguiente ejemplo a propósito de las redes sociales: una persona puede considerar excesivo tener que recurrir al juez por el solo hecho de que se le ha denegado alguno de los derechos de acceso,

[56]HERRERA, 2016, 106.
[57]PICA y VARGAS, 2021, 265.
[58]BECERRA, 2013, 186.
[59]SANZ, 2023, 9.

rectificación, cancelación y oposición, lo que tiene como consecuencia la impunidad de los presuntos responsables y, además, el incumplimiento del objetivo central de la referida normativa (es decir, el de garantizar el respeto y protección de la privacidad y los datos personales)[60]. Con la creación de la Agencia de Protección de Datos Personales (APDP) por parte de la Nueva LPDP, se genera un cambio de paradigma en esta materia.

En cuanto a sus orígenes, una primera virtud atribuible a la APDP es la de ser un organismo distinguible de otros, superándose así la intención presente en diversos proyectos de ley por radicar la función de resguardo de la información en la Contraloría General de la República, el Servicio Nacional del Consumidor, el Consejo para la Transparencia o el Servicio de Registro Civil.

En relación con las características generales de la APDP, y teniendo como objetivo central la obligación de velar por la "efectiva protección de los derechos que garantizan la vida privada de las personas y sus datos personales"[61], el carácter especializado de la Agencia, junto con sus facultades, se encuentra incorporado en los artículos 30 y 30 bis de la señalada ley[62]. En este sentido, respecto de su naturaleza jurídica, la APDP es una corporación autónoma de derecho público, de carácter técnico, descentralizado, con personalidad jurídica y patrimonio propio[63]. En lo concerniente al amplio espectro de facultades concedidas por la Nueva LPDP a la Agencia, estas pueden sistematizarse en cuatro categorías, destacándose en cada una de estas las siguientes atribuciones:

a) Facultades de proposición e interpretación normativa: incluye la potestad de dictar instrucciones y normas generales y obligatorias, con el fin de regular las operaciones de tratamiento de datos personales conforme con los principios establecidos en la Nueva LPDP. Además, tiene la facultad de aplicar e interpretar administrativamente las disposiciones legales y reglamentarias en materia de protección de los datos personales, y las instrucciones y normas generales que dicte la APDP[64].
b) Facultades de promoción y protección de los derechos sobre datos personales: comprende la facultad de resolver las solicitudes y reclamos que formulen los titulares de datos, en contra de quienes traten datos personales con infracción a la Nueva LPDP, sus reglamentos, instrucciones y normas dictadas por la Agencia. Igualmente, tiene la

[60]HERRERA, 2016, 103.

[61]Artículo 30, inciso 2, Nueva LPDP.

[62]Todos los aspectos vinculados con la APDP se encuentran en el "Título VI. Autoridad de Control en materia de Protección de datos personales" de la Nueva LPDP (entre los artículos 30 a 32 bis. inclusive).

[63]Artículo 30, inciso 1, Nueva LPDP.

[64]Artículo 30 bis, letras a) y b), Nueva LPDP.

facultad de desarrollar programas, proyectos y acciones de difusión, promoción e información a la ciudadanía, en relación con el respeto a la protección de sus datos personales[65].

c) Facultades fiscalizadoras y sancionatorias: incluyen la atribución de fiscalizar el cumplimiento de las disposiciones de la Nueva LPDP, sus reglamentos, instrucciones y normas que se dicten respecto de los tratamientos de datos personales. Simultáneamente, tiene la facultad de determinar las infracciones e incumplimientos en que incurran quienes realicen tratamiento de datos personales, en sus operaciones de tratamiento de datos, respecto de los principios y obligaciones establecidos en esta ley, sus reglamentos y las instrucciones y normas generales que emita la Agencia. Finalmente, posee el ejercicio de la potestad sancionadora sobre las personas naturales o jurídicas que infrinjan la Nueva LPDP [66].

d) Facultades consultivas: entre estas, se destaca la facultad de prestar asistencia técnica a un amplio espectro de autoridades del Estado. El objeto de esta atribución consiste en que las operaciones y actividades de tratamiento de datos personales realizadas por estos organismos se lleven a cabo conforme con los principios y obligaciones establecidos en la Nueva LPDP[67].

Ciertamente, la extensa gama de atribuciones entregadas por la ley a la APDP, concede a esta autoridad el carácter especializado exigido para enfrentar los retos que supone el uso de internet y las redes sociales: el conocimiento técnico y normativo de la Agencia es clave para lograr la efectiva aplicación de la Nueva LPDP en esos ámbitos del progreso informático. Simultáneamente y desde un punto de vista práctico, una labor exitosa por parte de la APDP con base en el ejercicio de sus facultades (como por ejemplo las fiscalizadoras y sancionatorias), permitirá al titular evitar las dificultades y demoras que implica acudir a la jurisdicción ordinaria.

Finalmente, anticipar los desafíos que pueda encontrar la Agencia chilena con ocasión del ejercicio de sus competencias, exige analizar la experiencia de organismos encargados del tratamiento de la información personal en el derecho comparado. Bajo esta premisa, tenemos el caso de la Agencia Española de Protección de Datos AEPD[68], autoridad de naturaleza independiente y garante de la tutela de esa información. Este organismo posee atribuciones oficiosas de control, instrucción y sanción,

---

[65]Artículo 30 bis, letras f) y g), Nueva LPDP.

[66]Artículo 30 bis, letras c), d) y e), Nueva LPDP.

[67]Las autoridades que incluye la norma son el Congreso Nacional, Poder Judicial, Contraloría General de la República, Ministerio Público, Tribunal Constitucional, Banco Central, Servicio Electoral, Justicia Electoral y "los demás tribunales especiales creados por ley". Artículo 30 bis, letra i), Nueva LPDP.

[68]Creada mediante la Ley Orgánica 5/1992, de 29 de octubre.

sin perjuicio de que el titular puede accionar en sede jurisdiccional para obtener resarcimiento patrimonial[69]. En lo que concierne a su rol en materia de protección de datos en las redes sociales (teniendo como precedente el caso Bodil Lindqvist[70], generador a su vez del estándar Lindqvist[71]), la autoridad española ha desarrollado diversas acciones, las que incluyen la promoción y participación en estudios, emisión de informes y aplicación del régimen sancionador.

Recientemente (2022) y en cuanto al régimen sancionador, casos como la denuncia por difusión masiva de un video grabado sin consentimiento de la víctima en redes sociales (concretamente Facebook), procedimiento identificado con el número de expediente EXP202204530[72], y en el que la AEPD impuso una sanción de 10.000 € a una persona física, permitió abrir el debate acerca de si en la conducta denunciada era aplicable el artículo 2 numeral 2 letra c) del GDPR, norma conforme a la cual el Reglamento europeo no se aplica al tratamiento de datos personales "efectuado por una persona física en el ejercicio de actividades exclusivamente personales o domésticas". En lo central, la relevancia de la decisión en comento radica en reconocer que el GDPR es aplicable, si las imágenes y videos compartidos en las plataformas informáticas permiten identificar a las personas afectadas, adquiriendo la información divulgada en la red el carácter de dato personal. La experiencia de este caso es útil pensando en la probable ocurrencia de una situación similar en Chile, teniendo en cuenta que la Nueva LPDP en su artículo 1º inciso final indica que sus normas no se aplican respecto del "tratamiento de datos que efectúen las personas naturales en relación con sus actividades personales".

c. *TRATAMIENTO DE LOS DATOS PERSONALES CONTENIDOS EN LAS REDES SOCIALES Y EL CONSENTIMIENTO*

Al tenor de lo ordenado en los incisos 1º y 2º del artículo 4 de la LPD, los datos personales del usuario de una red social pueden tratarse cuando el "titular consienta expresamente en ello", consentimiento que debe constar por escrito[73]. Igualmente, de acuerdo con ese estatuto dicho tratamiento

---

[69]BECERRA, 2013, 186.

[70]Sentencia del Tribunal de Justicia de 6 de noviembre de 2003, en el asunto C-101/01. Bodil Lindqvist fue acusada de haber infringido la normativa sueca relativa a la protección de datos personales, por motivos de publicar en su sitio web diversos datos de carácter personal de varios individuos, los que colaboraban junto a ella en una parroquia. La señora Lidqvist no había informado a sus compañeros de la existencia de esta página web. Tras ser sancionada y recurrir, el tribunal sueco consultó al Tribunal de Justicia acerca de las condiciones de aplicación de la Directiva 95/46/CE. Al final, el Tribunal consideró que la citada Directiva era aplicable al caso.

[71]RALLO y MARTÍNEZ, 2011, 42.

[72]AEPD, Expediente N.º: EXP202204530, Resolución de Procedimiento Sancionador, 08/03/2022.

[73]HERRERA, 2016, 98.

es posible cuando la ley lo autorice[74]. A este respecto, un problema identificado en la LPD es la falta de definición de lo que se debe entender por "consentimiento". Asociada a la anterior situación, la manifestación del consentimiento en las redes sociales es insuficiente para cumplir con las exigencias de la citada ley. Con el siguiente ejemplo, Herrera visualiza esta problemática[75]: Facebook señala que el contrato suscrito entre el usuario y la red social, se perfecciona en el momento en que el internauta pulsa el botón de registro. De esta manera, al hacer clic el usuario se somete a un contrato de adhesión[76], aceptando las condiciones y políticas de privacidad de la plataforma tecnológica. Así, este acto es insuficiente para considerar que el consentimiento fue otorgado de forma "libre, expresa y por escrito". Igualmente, es discutible pensar que dicho consentimiento tiene un carácter inequívoco e informado: en efecto, en general los usuarios potenciales de la red social carecen de interés por leer las políticas de privacidad y condiciones de uso, debido a su extensión y complejidad[77].

Por su parte, la Nueva LPDP consagra la definición del "consentimiento" en su artículo 2, letra p). Esta definición se complementa con lo establecido en el artículo 12 de la señalada ley, disposición que explica las características, formalidades, posibilidad de mandato y exigencias para la revocación del consentimiento. En este orden de ideas, al combinar las normas anteriores observamos que el consentimiento, como requisito para que el tratamiento de los datos personales tenga un carácter lícito, es toda manifestación de voluntad libre, específica (en cuanto a su finalidad o finalidades), expresa, previa, inequívoca e informada. Respecto de su formalidad, este consentimiento se debe manifestar mediante una declaración verbal, escrita o expresada por un medio electrónico equivalente, o "mediante un acto afirmativo que dé cuenta con claridad de la voluntad del titular"[78], estableciéndose además la posibilidad que un mandatario otorgue el consentimiento. En relación con la *revocación*, el titular puede revocar el consentimiento en "cualquier momento y sin expresión de causa, utilizando medios similares o equivalentes a los empleados para su otorgamiento"[79], revocación que no tiene efectos retroactivos. Igualmente,

---

[74]LARA y otros, 2014, 34.

[75]HERRERA, 2016, 98.

[76]Se dice que es un contrato de adhesión, ya que el contenido de las cláusulas es establecido de forma unilateral por la plataforma informática. DE LA MAZA, a propósito de los contratos por adhesión en plataformas electrónicas en el caso chileno, ha reconocido como riesgo de estos contratos la incorporación de cláusulas abusivas, es decir, de aquellas que generan desequilibrios significativos en perjuicio de la parte que no redactó el acto. DE LA MAZA, 2005, 286.

[77]CÁRDENAS y MATÍAS, 2025, 30.

[78]Respecto del "acto afirmativo que dé cuenta con claridad de la voluntad del titular", corresponde a la doctrina establecer los "actos" que pueden tener esta calidad.

[79]El artículo 12 inciso 5º de la Nueva LPDP se extiende en este punto, indicando que "los medios utilizados para el otorgamiento o la revocación del consentimiento deben ser expeditos, fidedignos, gratuitos y estar permanentemente disponibles para el titular".

la norma presume que el consentimiento para tratar datos no ha sido libremente otorgado[80], "cuando el responsable lo recaba en el marco de la ejecución de un contrato o la prestación de un servicio en que no es necesario efectuar esa recolección"[81].

En conclusión, la Nueva LPDP al exigir expresamente que el tratamiento de la información dependa del consentimiento "expreso, previo, libre, inequívoco e informado" por parte del titular, apunta en la dirección correcta con el fin de reducir la asimetría en la relación entre el usuario y la plataforma informática. Finalmente, y a partir de la implementación efectiva de la norma, son varios los retos a superar para la aplicación adecuada del consentimiento. El primer desafío es la problemática inherente al consentimiento en bloque, donde la recomendación es que los responsables de datos eviten exponer sus políticas de privacidad y tratamiento de la información en bloque. Simultáneamente, para el usuario se deben generar aceptaciones independientes asociadas a finalidades específicas (o consentimiento granular[82]). Un segundo reto lo constituye la necesidad de contar con más alternativas frente al modelo *Pay or Consent*, arquetipo que ofrece al usuario dos opciones: usar un servicio de forma gratuita y otorgar su consentimiento para tratar sus datos y realizar publicidad comportamental, o pagar una tarifa por el servicio sin publicidad.

Frente a las opciones limitadas que ofrece el modelo *Pay or Consent* al titular de los datos, se puede aprovechar la experiencia del Comité Europeo de Protección de Datos (CEPD), pensando en el caso chileno. En efecto, recientemente este Comité (2024) ha dictaminado que, en general, los responsables del tratamiento tienen la responsabilidad de crear y documentar un proceso de información "que permita a los interesados tener una comprensión completa y clara del valor, el alcance y las consecuencias de sus posibles elecciones". Bajo esta premisa, el organismo europeo señala que estos responsables deben ofrecer más alternativas para asegurar la libertad del consentimiento, incluyendo opciones que no impliquen el pago de una tasa o precio, y que permitan una forma de publicidad con el tratamiento de menos o ningún dato personal[83].

---

[80]Esta hipótesis de presunción de falta de libertad se puede presentar cuando estamos frente a las "ventas atadas", figura que en el ámbito negocial transcurre entre las prácticas anticompetitivas y la violación de los derechos del consumidor. ALVIRA y GONZÁLEZ, 2019, 131.

[81]Siguiendo con el caso de las "ventas atadas", en ellas el titular no puede contratar sin antes aceptar el tratamiento de sus datos personales, incluso para fines que van más allá del servicio contratado.

[82]El "consentimiento granular" permite a los usuarios elegir qué tipos de tratamientos de sus datos personales desean aceptar, en lugar de verse obligados a aceptar o rechazar todas las condiciones de manera conjunta. OBSERVATORIO DE DATOS PERSONALES (2024).

[83]El CEPD adoptó un dictamen a raíz de una solicitud del artículo 64, apartado 2, del GDPR presentada por las autoridades neerlandesas, noruegas y de Hamburgo para la protección de datos. El dictamen, aborda la validez del consentimiento para tratar datos personales con fines de publicidad comportamental, en el contexto de modelos de consentimiento o pago

d. *INFORMACIÓN PERSONAL VERTIDA EN LAS REDES SOCIALES Y CONCEPTO DE "FUENTE DE ACCESO PÚBLICO"*

A la luz de la LPD y en relación con la información personal vertida en las redes sociales, se ha reflexionado acerca de los efectos de una inadecuada configuración de privacidad por parte del usuario al momento del efectuarse el registro en una red social. En este caso, Herrera admite la posibilidad que esa información pueda ser considerada como "fuente de acceso público"[84]. Desde esta perspectiva, otro ámbito de la LPD donde es posible identificar un elemento de naturaleza deficiente, tiene que ver con las situaciones en las que no se requiere autorización para el tratamiento de datos. Al respecto, los incisos 5º y 6º del artículo 4º de la señalada Ley consagran diversas excepciones, en relación con la autorización del titular requerida para el tratamiento de la información personal. El inciso 5º establece la posibilidad de llegar a esa información cuando el dato se encuentra en una fuente accesible al público. El problema identificado en este punto surge a partir de la definición que la Ley [artículo 2 letra i), LPD] otorga a esta fuente: "los registros o recopilaciones de datos personales públicos o privados, de acceso no restringido o reservado a los solicitantes".

En este sentido, Anguita[85] opina que la ambigüedad de esta definición determina cómo, a menos que el titular de la información permita su divulgación, o a menos que la ley prohíba expresamente esa divulgación, cualquiera puede dar tratamiento a la información que se encuentra en esta *fuente*. Por tanto, y aplicando las definiciones y excepciones de la LPD, los datos incorporados en las redes sociales (y en general la información contenida en internet) se convierten en una información accesible al público. Al final, en este caso estamos ante una excepción tan amplia que termina transformando la desprotección en la regla general.

Con la Nueva LPDP, se avanza en la superación de la ambigüedad atribuida a la noción de fuente accesible al público de la LPD. A este respecto, la ley de protección de datos recién aprobada define cuáles *fuentes* tienen este carácter, indicando que son "todas aquellas bases de datos o conjuntos de datos personales, cuyo acceso o consulta puede ser efectuada en forma lícita por cualquier persona, tales como el Diario Oficial, medios de comunicación o los registros públicos que disponga la ley"[86]. No obstante,

---

desplegados por las grandes plataformas en línea. COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (2024).

[84]HERRERA, 2016, 101.

[85]Incluso autores como Anguita Ramírez, al criticar la ambigüedad de la definición de "fuente accesible al público", considera esta descripción como la más desafortunada de la LPD en comparación con otras normas equivalentes. ANGUITA, 2007, 295-296.

[86]Por cierto, la norma encargada de este tema [artículo 2, letra j), Nueva LPDP] concluye indicando que "El tratamiento de datos personales provenientes de fuentes de acceso público se someterá a las disposiciones de esta ley".

un aspecto a tener en cuenta es que la Nueva LPDP, aunque establece un listado de bancos que pueden ser fuentes de acceso público (lo que no ocurría en la LPD), este listado no tiene un carácter taxativo. Lo anterior, se deduce del uso de la expresión "tales como", otorgándole entonces a esta enumeración el carácter de ejemplos ("Diario Oficial, medios de comunicación o los registros públicos que disponga la ley"). Respecto de este punto compartimos la opinión de Alvarado, quien insiste en la conveniencia de que las leyes pertinentes a protección de datos incorporen un catálogo cerrado de bancos de datos, susceptibles de ser considerados como fuentes accesibles al público. Lo anterior (agrega el mismo autor), con el fin de evitar generar incertidumbre para el titular de esos datos, al permitirse tratamientos sin su consentimiento: al dejar un catálogo abierto, se puede entrar en la discusión acerca de si esta categoría responde a una situación de hecho, o a una determinación normativa[87].

Para finalizar esta parte y a propósito de la experiencia comparada, un aspecto interesante es que, no obstante el GDPR admite la posibilidad de recolección de datos de "fuentes de acceso público" [artículo 14, número 2, letra f), GDPR][88], el Reglamento europeo no señala expresamente qué *fuentes* tienen la calidad de ser accesibles al público. Lo anterior, pese a que en el caso español la Ley Orgánica 15/1999 (o LOPD 15/1999) definía y señalaba inequívocamente cuáles eran estas fuentes[89]. Ahora bien, frente al hecho que la Ley Orgánica 3/2018 (o LOPD 3/2018, estatuto que derogó la LOPD 15/1999) carece de estas definiciones (ausencia que, insistimos, también se observa en el GDPR), la Agencia Española de Protección de Datos (AEPD) ha estimado que es posible seguir aplicando como criterio interpretativo la Ley Orgánica derogada, otorgando el carácter de "fuentes de acceso público" a las páginas web y fuentes que pueden ser objeto de libre consulta, excluyéndose el acceso a los sitios restringidos a un círculo determinado de usuarios[90]. En este orden de ideas, debido a que la Nueva LPDP chilena sí define las fuentes de acceso público e incorpora

[87]ALVARADO, 2014, 221.

[88]A propósito de la información que se debe facilitar cuando los datos personales no se han obtenido del interesado, y conforme con lo estipulado en el artículo 14 número 2 letra f) del GDPR, se impone al responsable del tratamiento la obligación de indicar la fuente de la que proceden los datos personales y, en su caso, si proceden de fuentes de acceso público.

[89]En efecto, el artículo 3, letra j) de la LOPD 15/1999 indicaba "Fuentes accesibles al público: aquellos ficheros cuya consulta puede ser realizada, por cualquier persona, no impedida por una norma limitativa o sin más exigencia que, en su caso, el abono de una contraprestación. Tienen la consideración de fuentes de acceso público, exclusivamente, el censo promocional, los repertorios telefónicos en los términos previstos por su normativa específica y las listas de personas pertenecientes a grupos de profesionales que contengan únicamente los datos de nombre, título, profesión, actividad, grado académico, dirección e indicación de su pertenencia al grupo. Asimismo, tienen el carácter de fuentes de acceso público los diarios y boletines oficiales y los medios de comunicación".

[90]GRUPO ADAPTALIA (2019).

un listado de bancos que pueden tener la calidad de fuentes, se le atribuye una fortaleza en comparación con la norma europea.

VI. CONCLUSIONES

1. A nivel universal, una de las consecuencias de los avances en el ámbito de las telecomunicaciones y la informática, es su impacto en la modificación de la conducta de los individuos dentro del espectro de internet. Chile no ha sido ajeno a esta influencia y sus efectos, lo que involucra a las redes sociales.
2. Aproximarnos a los avances de la nueva LPDP en su relación con las redes sociales exigió, como punto de partida, comentar las dificultades en el proceso de redacción y las fallas atribuidas a la LPD, anomalías que justificaron la redacción del nuevo marco legal en materia de protección de datos.
3. Respecto de las redes sociales y su impacto en el tratamiento de la información personal (y con independencia de la definición que se acoja de estas estructuras formadas en la esfera de internet) se concluye que, de los elementos que configuran una red social capaces de generar las mayores vulneraciones a la privacidad o a los datos personales (comunicación, identidad e interconectividad), del elemento "identidad" emergen las principales transgresiones contra el derecho a la tutela de la información personal. Lo anterior, teniendo en cuenta que los datos personales que conforman la personalidad del individuo son el medio de cambio para poder ingresar y participar en estas redes.
4. Como un aspecto complementario en la investigación, se abordó el tratamiento de la "expectativa de privacidad" asociada a las plataformas informáticas, desde la perspectiva de la jurisprudencia de la CS. Acerca de este asunto, en materia resolución de acciones de protección constitucional vinculadas a publicaciones en redes sociales, se observa que en las decisiones de la CS no hay un empleo del derecho a la tutela de los datos personales, salvo alusiones tangenciales. Igualmente, al contrastar la casuística vinculada a diferentes plataformas informáticas, la conclusión es que los argumentos de la CS para reconocer o no la expectativa de privacidad, dependerán de la renuncia tácita a mantener una esfera privada o íntima (como ocurre con Facebook), a la aceptación voluntaria de compartir cierta información (como sucede con Grindr), o a la confianza en la existencia de una seguridad predetermina capaz de proteger lo transmitido (como ocurre con WhatsApp).
5. La labor de contraste entre la LPD y la Nueva LPDP evidencia cambios respecto del tratamiento de la información personal dentro de las redes

sociales. Estos cambios implican progresos en la superación de las fallas atribuidas a la LPD, escenario que involucra diversas áreas:

5.1. El tratamiento de los datos personales de los menores de edad (en general), y su efecto en las redes sociales (en particular), es uno de los aspectos de mayor avance normativo. En efecto, mientras que la LPD no concede una protección especial a la información personal de este grupo vulnerable, la Nueva LPDP da tratamiento expreso a los datos personales "relativos a los niños, niñas y adolescentes (artículo 16 quáter)". Como elemento clave para alcanzar un mayor estándar de protección de este grupo etario, la nueva ley exige el otorgamiento del consentimiento de los padres o representes de los niños y niñas para el tratamiento de la información personal, y el otorgamiento del consentimiento de los padres o representes de los adolescentes para el tratamiento de los datos personales sensibles. Desde el punto de vista de las redes sociales, esta exigencia pretende combinar de forma armónica el interés superior de los menores de edad, con la autonomía que van adquiriendo a medida que desarrollan su identidad, con la finalidad de un disfrute más seguro de las actividades desarrolladas en el ámbito de internet.

5.2. Como vacío estructural, a la LPD se le critica la falta del reconocimiento de un organismo con la capacidad de regular el tratamiento de la información personal. Esta ausencia termina por constreñir al titular afectado con la utilización indebida de sus datos (hipótesis que incluye el mal uso de la información incorporada en las redes sociales) a recurrir a la jurisdicción ordinaria, con todos los costos y complejidades inherentes a estos procedimientos. La Nueva LPDP genera un cambio de paradigma, con la creación de la Agencia de Protección de Datos Personales (APDP), autoridad independiente que cuenta con un amplio rango de competencias (artículos 30 y 30 bis). Este espectro de atribuciones se puede sistematizar en cuatro categorías, que incluyen facultades de proposición e interpretación normativa, atribuciones de promoción y protección de los derechos sobre datos personales, facultades fiscalizadoras y sancionatorias, y competencias consultivas. La extensa gama de atribuciones entregadas por la Nueva LPDP a la APDP, otorga a este organismo el carácter especializado exigido para asumir los retos que supone el uso de internet y las redes sociales. Finalmente, y con el propósito de anticipar los desafíos a los que se puede enfrentar la APDP chilena con ocasión del ejercicio de sus competencias, se sugiere tomar en cuenta la experiencia de organismos encargados del tratamiento de la información personal en el derecho comparado, en particular la AEPD.

5.3. A propósito del consentimiento exigido para el tratamiento de los datos personales, un problema identificado en la LPD es su falta

de definición. Asociada a esta ausencia conceptual, la doctrina explica que la sola manifestación del consentimiento en las redes sociales es insuficiente, para considerarlo otorgado de forma "libre, expresa y por escrito" (razón por la cual en este caso no se cumplen los requisitos exigidos por la misma ley). En contraste, con la Nueva LPDP estas deficiencias son superadas. En efecto, la norma estipula de forma clara la definición de consentimiento [artículo 2, letra p)], noción que reconoce en esta manifestación de voluntad su naturaleza libre, específica (en cuanto a su finalidad o finalidades), expresa, previa, inequívoca e informada. Esta noción es complementada con una descripción de sus características, formalidades, hipótesis de mandato y exigencias para la revocación (artículo 12). Concluimos que, con la aplicación combinada de los anteriores elementos, la Nueva LPDP apunta en la dirección correcta, con el fin de reducir la asimetría en la relación entre el usuario y la plataforma informática. De todas formas y a partir de la implementación efectiva de la norma, son varios los desafíos a superar para la aplicación adecuada del consentimiento, escenario que incluye la problemática inherente al consentimiento en bloque, y la necesidad de contar con más alternativas frente al modelo *Pay or Consent*, retos respecto de los cuales formulamos una serie de recomendaciones en la investigación.

6. Finalmente, a la luz de la LPD, frente a la hipótesis de una inadecuada configuración de privacidad al momento de efectuarse el registro en una red social, la doctrina admite la posibilidad que la información personal vertida en la plataforma informática se pueda considerar como fuente de acceso público. En este caso, a propósito de las situaciones en las que no se requiere autorización para el tratamiento de datos (situaciones que deben tener, al menos en teoría, un carácter excepcional), criticamos el carácter ambiguo de la definición de fuente accesible al público consagrada en el artículo 2 letra i) de la LPD, ya que como efecto de esta ambigüedad los datos incorporados en las redes sociales (y en general la información contenida en internet) se convierten en información accesible al público, caso en el que estaríamos ante una excepción tan amplia que termina transformando la desprotección en la regla general. La Nueva LPDP establece un listado de bancos que pueden ser *fuentes* (lo que no ocurre en la ley anterior), factor que determina un avance en la superación de la ambigüedad atribuida a la noción de fuente accesible al público de la LPD. No obstante, este listado no tiene un carácter taxativo, es decir, constituye un catálogo abierto. Para la literatura jurídica, lo ideal es que la norma incorpore un catálogo cerrado de bancos de datos, con el fin de evitar generar incertidumbre para el titular de la información, ya que se podrían originar tratamientos sin su consentimiento: al dejar

un catálogo abierto, existe la posibilidad de entrar en la discusión acerca de si esta categoría responde a una situación de hecho, o a una determinación normativa.

VII. REFERENCIAS BIBLIOGRÁFICAS

I. DOCTRINA

AGUSTINOY GUILAYN, Albert. y MONCLÚS RUIZ, Jorge (2016): Aspectos legales de las redes sociales. Barcelona, Editorial Wolters Kluger, primera edición.

ALVARADO, Francisco (2014): "Las fuentes de acceso público a los datos personales", Revista Chilena de Derecho y Tecnología, 3 (2), 205-226 (DOI: https://doi.org/10.5354/0719-2584.2014.33276).

ALVIRA ARBELÁEZ, Felipe y GONZÁLEZ VARELA, Santiago (2019): "La venta atada como práctica anticompetitiva y vulneración al derecho del consumidor", *Revista de derecho de la competencia,* CEDEC (Nº. Extra 1), 131-160.

ANGUITA RAMÍREZ, Pedro (2007): La protección de datos personales y el derecho a la vida privada, régimen jurídico, jurisprudencia y derecho comparado. Santiago, Editorial Jurídica de Chile.

BECERRA POBLETE, Pablo (2013): "Potestades sancionatorias en el proyecto de reforma a la Ley Nº 19.628 de Protección de Datos personales. Una crítica", *Revista de Derecho*, Escuela de Postgrado (3), 63-192 (DOI: https://doi.org/10.5354/rdep.v0i3.31017).

CÁRDENAS OYARZÚN, Héctor y URIBE CONEJEROS, Matías (2025): "La protección de datos personales tras la Ley 21.719: Implicancias regulatorias y proyecciones para las empresas en las relaciones laborales", *Revista de Derecho Aplicado* LLM UC, 15, 1-42 (DOI: https://doi.org/10.7764/rda.15.91346).

COMITÉ EUROPEO DE PROTECCIÓN DE DATOS (en línea), Dictamen 8/2024 sobre el consentimiento válido en el contexto de los modelos de consentimiento o pago aplicados por las plataformas en línea de gran tamaño, Adoptado el 17 de abril de 2024. Disponible en internet: https://www.edpb.europa.eu/system/files/2024-11/edpb_opinion_202408_consentorpay_es.pdf.

CONTRERAS, Pablo y LOVERA, Domingo (2021): "Redes sociales, funas, honor y libertad de expresión: análisis crítico de los estándares de la jurisprudencia de la Corte Suprema chilena", Derecho PUCP, (87), 345-371 [DOI: http://dx.doi.org/10.18800/derechopucp.202102.010].

CONTRERAS, Pablo (2020): "El derecho a la protección de datos personales y el reconocimiento de la autodeterminación informativa en la Constitución chilena", *Estudios Constitucionales*, 18 (2), 87-120 (DOI: 10.4067/S0718-52002020000200087).

CONTRERAS, Pablo y LOVERA, Domingo (2020): *La Constitución de Chile*. Valencia, Tirant lo Blanch.

DE LA CUADRA, Elena (1996): "Internet: conceptos básicos", Cuaderno de orientación multimedia, 5, 35-56. Disponible en: https://core.ac.uk/download/pdf/153334271.pdf.

DE LA MAZA, Íñigo (2005): "Los contratos por adhesión en plataformas electrónicas: una mirada al caso chileno", *SCRIPT-ed*, 2 (3), 283-289.

DIARIO CONSTITUCIONAL (18 de octubre de 2021): "Acceso a redes sociales: menores de 14 años deberán contar con autorización de sus padres". Disponible en https://www.diarioconstitucional.cl/2021/10/18/acceso-a-redes-sociales-menores-de-14-anos-deberan-contar-con-autorizacion-de-sus-padres/.

ESCOBAR VEAS, Javier (2023): "Redes sociales y expectativa legítima de privacidad en la jurisprudencia de la Corte Suprema chilena", *Revista Chilena de Derecho y Tecnología*, 12, 1-25 (DOI: https://doi.org/10.5354/0719-2584.2023.69893).

GRUPO ADAPTALIA (29 de julio de 2019): "Fuentes de Acceso Público en la LOPD y el RGPD". Disponible en: https://grupoadaptalia.es/blog/fuentes-de-acceso-publico-en-la-lopd-y-el-rgpd-2/.

HERRERA CARPINTERO, Paloma (2016): "El derecho a la vida privada y las redes sociales en Chile", *Revista Chilena de Derecho y Tecnología*, 5 (1), 87-112 (DOI: http://dx.doi.org/10.5354/0719-2584.2016.41268).

HUERTA, Gustavo, TORRES, Carlos y LAGUNES, Agustín (2021): "Identidad digital en el ámbito educativo", en TORRES, Carlos y LAGUNES, Agustín (coordinadores), *Sistemas y ambientes educativos: estado del conocimiento*. Veracruz-México, Universidad Veracruzana, 46-61.

JIJENA LEIVA, Renato (1992): *La protección penal de la intimidad y el delito informático*. Santiago, Editorial Jurídica de Chile.

LARA, Carlos, PINCHEIRA, Carolina y VERA, Francisco (2014): "La privacidad en el sistema legal chileno", Policy Papers, ONG Derechos Digitales (8), 1-93.

MARIKO, Hirose (2017): "Privacy in public spaces: The reasonable expectation of privacy against the dragnet use of facial recognition technology", Connecticut *Law Review*, 49 (5), 1591-1620.

MILANÉS, Valeria (2017): "Desafíos en el debate de la protección de datos para Latinoamérica", *Revista Transparencia & Sociedad del Consejo para la Transparencia* (5), 13-31.

NIEVES SALDAÑA, María (2007): "La protección de la privacidad en la sociedad tecnológica: el derecho constitucional a la privacidad de la información personal en los Estados Unidos", *Araucaria Revista Iberoamericana de Filosofía, Política y Humanidades*, 18 (2), 85-115.

NOVOA MONREAL, Eduardo (2001): *Derecho a la vida privada y libertad de información: un conflicto de derechos*. México DF., Siglo XXI, sexta edición.

OBSERVATORIO DE DATOS PERSONALES (30 de agosto del 2024): "La importancia de los consentimientos granulares, no vale un «vale para todo". Disponible en: https://datos.personales.es/la-importancia-de-los-consentimientos-granulares-no-vale-un-vale-para-todo/#:~:text=El%20consentimiento%20granular%20permite%20a,las%20condiciones%20de%20manera%20conjunta.

ONG META (2012): Minuta sobre modificaciones a Ley Nº 19.628, sobre protección de la vida privada y protección de datos de carácter personal, Santiago, ONG META.

ORDOÑEZ PINEDA, Luis y CALVA JIMÉNEZ, Stefany (2020): "Amenazas a la privacidad de los menores de edad a partir del *sharenting*", *Revista Chilena de Derecho y Tecnología*, 9 (2), 105-130 (DOI: http://orcid.org/0000-0002-0262-2212).

PÉREZ GÓMEZ, Ángel (2013): "Educarse en la era digital. Adelanto del nuevo libro de Ángel Pérez Gómez (Separata)", *Sinéctica*, 40 (1), 47-72.

PICA, Rodrigo y VARGAS, Matías (2021): "Desafíos del derecho de protección de datos personales y la autodeterminación informativa en Chile", en SERRANO

MAILLO, María Isabel (directora), *El Derecho a la protección de datos personales en Europa y en América: diferentes visiones para una misma realidad*. Tirant lo Blanch), 235-275.
RALLO, Artemi y MARTÍNEZ, Ricard (2011): "Protección de datos personales y redes sociales: obligaciones para los medios de comunicación", *Quaderns del CAC* 37, XIV (2), 41-51.
RIVERA RESTREPO, José (2022): "La autonomía progresiva de los niños, niñas y adolescentes en el Proyecto de Constitución Política de la República de Chile de 2022", Revista de Derecho y Ciencias Sociales, (26), 145-159.
SÁEZ, Raúl (2010): "La OCDE y el ingreso de Chile", *Estudios Internacionales*, 43 (166), 93-112 (DOI: https://doi.org/10.5354/0719-3769.2010.12670).
SANZ SALGUERO, Francisco (2025): "Tutela de la información personal: desafíos para la protección de los datos biométricos en Chile", *Revista Ius et Praxis*, 31 (2), 3-23 (DOI: 10.4067/S0718-0012202500020000).
SANZ SALGUERO, Francisco (2023): "Desafíos para la modernización de la Ley Nº 19.628 de 1999, de cara al alcance extraterritorial del Reglamento General de Protección de Datos de la Unión Europea GDPR", *Revista CES Derecho*, 14 (1), 3-16. (DOI: https://doi.org/10.21615/cesder.6806).
SANZ SALGUERO, Francisco (2018): "Delimitación de las esferas de la vida privada, privacidad e intimidad, frente al ámbito de lo público", *Revista Transparencia & Sociedad del Consejo para la Transparencia* (6), 127-149.
SANZ SALGUERO, Francisco (2013): "Solicitud de acceso a la información y tutela de los datos personales de un tercero", *Revista de Derecho de la Pontificia Universidad Católica de Valparaíso*, 41 (2), 457-502 (DOI: http://dx.doi.org/10.4067/S0718-68512013000200014).
SCAFFIDI RUNCHELLA, Livio (2021): "Pubblicazione e condivisione di foto sui social network: la tutela del minore fra diritto all'immagine e protezione dei dati personali", *Freedom, Security & Justice: European Legal Studies* (3), 282-315 (DOI: 10.26321/L.SCAFFIDI.RUNCHELLA.03.2021.12).
SCHWARTZ, Paul (2000): "Internet, Privacy and the State", *Connecticut Law Review*, 32, 815-859.
SERRANO, María Isabel y MARTÍNEZ, Esther (2021): "La protección de los datos personales en la infancia y la adolescencia", en SERRANO MAILLO, María Isabel (directora), *El Derecho a la protección de datos personales en Europa y en América: diferentes visiones para una misma realidad*. Tirant lo Blanch, 579-617.
TORRES, Javiera (2021): "¿Las personas fallecidas tienen titularidad sobre el derecho a la privacidad?: una mirada en los tiempos de Facebook", en ROMERO, Sophia (coordinadora), *Justicia Electrónica*. Tirant lo Blanch, 221-232.
VIOLLIER, Pablo (2017): *El estado de la protección de datos personales en Chile*. Santiago de Chile, Derechos Digitales.
WE ARE SOCIAL (July 21, 2022): "The global state of digital in july 2022 | part one". Disponible en: https://wearesocial.com/uk/blog/2022/07/the-global-state-of-digital-in-july-2022/.

II. NORMAS E INSTRUMENTOS CITADOS

Chile, Constitución Política de la República, 11 de agosto de 1980.

Chile, Ley 21.719: Regula la protección y el tratamiento de los datos personales y crea la Agencia de Protección de Datos Personales, 13 de diciembre de 2024.

Chile, Ley Nº 21.096: consagra el derecho a protección de los datos personales, 16 de junio de 2018.

Chile, Ley Orgánica 3/2018: de Protección de Datos Personales y garantía de los derechos digitales, 5 de diciembre de 2018.

Chile, Ley Nº 19.628: acerca de protección de la vida privada, 28 de agosto de 1999.

Unión Europea, Reglamento General de Protección de Datos (UE) Nº 2016/679, 27 de abril de 2016.

Unión Europea, Directiva 95/46/CE del Parlamento Europeo y del Consejo, relativa a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos, 24 de octubre de 1995.

III. JURISPRUDENCIA CITADA

A. Jurisprudencia Nacional citada

Corte Suprema, 26 de mayo de 2022, Rol. 12185-2022. Recurso de apelación.

Corte Suprema, 21 de abril de 2022, Rol 42718-2021, Recurso de nulidad.

Corte Suprema, 19 de abril de 2022, Rebolledo/Vargas, Inmobiliaria General Cruz SpA y Badía, Rol. 71491-2021. Recurso de protección.

Corte Suprema, 21 de diciembre de 2020, Rol. 104785-2020. Recurso de apelación.

Corte Suprema, 11 de diciembre de 2020, Godoy/Sepúlveda y Cancino, Rol 90737-2020. Recurso de protección.

Corte Suprema, 7 de agosto de 2020, Mendoza/Ramírez, Rol 58531-2020. Recurso de protección.

Corte Suprema, 5 de agosto de 2019, Rol. 20441-2018. Recurso de nulidad.

Corte Suprema, 8 de noviembre de 2018, Rol 16921-2018. Recurso de nulidad.

Corte Suprema, 28 de febrero de 2018, Rol 1067-2018, Recurso de nulidad.

Corte Suprema, 30 de agosto del 2012, Silva/ prefecto de la prefectura Cautín, Rol 5322-2012. Recurso de apelación.

B. Jurisprudencia extranjera citada

Agencia Española de Protección de Datos, Expediente Nº: EXP202204530, Resolución de Procedimiento Sancionador, 8/3/2022.

Tribunal de Justicia de la Unión Europea, 6 de noviembre del 2003, sentencia C-101/01.